RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: LAW-M01

Navigating the Legal Landscape: Cyber Law 2025

Julie Bowen
Senior VP, GC, and Corp. Sec'y
MITRE Corporation
jbowen@mitre.org

Rick Aldrich
Cybersecurity Policy & Compliance
Booz | Allen | Hamilton
Aldrich_Richard@bah.com
@AldrichRick

Aravind Swaminathan
Partner
Orrick
aswaminathan@orrick.com
@cyber_swami

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

- This presentation is designed to raise awareness of general legal principles raised in several recent domestic and foreign cyber-related cases
- This session, and any information contained in this presentation, should not be construed as legal advice*
- The views and opinions expressed in this presentation are those of the authors and do not necessarily reflect the policy, opinion, or position of their employers or any other entity.

* **Disclaimer:** Information contained herein, and in this briefing, is for informational purposes and general guidance on matters of interest only and should not be considered legal advice or a recommendation. The application and impact of laws can vary widely based on specific facts and jurisdictions. Given the changing nature of laws, rules and regulations, there may be omissions or inaccuracies in the information contained in this presentation. Nothing by the presenters or moderator, or the information presented herein, is intended for, nor should it be construed as, rendering legal advice or services. This should not be a substitute for consultation with professional legal advisers.

Theme: Many Voices. One Community

- Goal of this Session
  - Lawyers are one of the many voices
  - Oftentimes brought into the cybersecurity process too late
  - This session will highlight cases that emphasize the importance of including legal voices to make the community stronger

> “Alone we can do so little; Together we can do so much”
>
> Helen Keller

Chevron deference

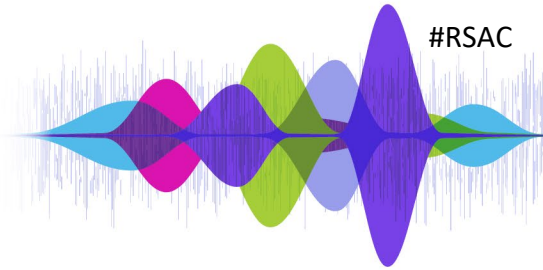
***Loper Bright Enterprises v. Raimondo*, 603 U.S. 369 (2024)**

- Facts of the case
- Issue: Should Court overrule or refine 30-year-old *Chevron* doctrine, that required courts to defer to Agency interpretations of statutes that are "silent or ambiguous" on the issue being reviewed?

Holding

- Overturned *Chevron* deference doctrine as a violation of 1946 Administrative Procedures Act by a 6-2 vote.
- Held APA requires courts to independently interpret statutes—not defer to federal agencies. Could result in splintered requirements
- Takeaway: Agency rulemaking in jeopardy
  - EPA, SEC, less likely to implement cybersecurity standards
  - CISA may be able to fill some gaps, but will get no deference
  - Congress will be challenged to fill gaps and respond to rapid changes in technology and cybersecurity

False Claims Act



***United States ex. Rel. Craig v. Georgia Tech*, No. 1:22-cv-02698-JPB (N.D. Georgia, 2024)**

- Facts of the case
- Issue: Does a DoD contractor's false assertion of compliance with contractual cybersecurity standards relating to the handling of sensitive information constitute a False Claims Act violation?

Holding

- Pending
  - U.S. DoJ intervened 22 Aug 24.
  - Alleged false cybersecurity assessment score of 98/110 (score submission was "condition of contract")
- Similar suit against Penn State was settled for $1.25M
- Allegedly 10 additional suits pending under seal
- Takeaway: DoJ's Civil Cyber-Fraud Initiative was actively pursuing these types of cases. Penalties could include sum of false invoices ($19M), plus penalties, treble damages. Unclear whether that will still be the case under the new Administration, but companies should review contracts, conduct internal compliance checks regularly, ensure staff is trained to comply and to alert.

Artificial Intelligence

***Ohio v. Tolbert*, CR-24-689572-A (Cuyo. Cty 2024)**

- Facts of case
- Issue: Does the use of AI-derived data in a search warrant justify suppression of the data in this case?

Holding

- Yes (but on appeal)
- Held search warrant failed to apprise judge that affidavit relied on AI facial recognition. Held akin to anonymous informant, so not enough for Probable Cause.
- Clearview AI clearly indicated its findings not “intended or permitted” to be used in any court filing.
- Takeaway: When using AI clearly indicate so, then augment with additional factors. Ensure your organization has guidelines for permitted and unpermitted uses of AI, and protections for corporate data.

"Reverse Warrants"

***United States v. Smith*, No. 23-60321, (5th Cir. 2024)**

- Facts of the case
- Issue: Are the use of geofence warrants a violation of the Fourth Amendment?

Holding

- 5th Cir: Yes (*contra* 4th Cir's holding in *Chatrie*)
- Held geofence warrants are akin to a general warrant. Analogized the S/C's concerns in *Carpenter* to the facts of this case.
- Disagreed with 4th Cir. that temporal limitation and "opt-in" to Google's Location History saved geofence warrants
- Takeaway: There is a split in the circuits that makes this issue ripe for S/C review. Use caution when using this or other types of reverse warrants. For those subject to reverse warrants, ensure clear guidelines on how to comply and whether retaining such data supports corporate goals and values.

Cases to Watch

- *United States v. Hasbajrmi*, No. 1:11-cr-623 (E.D.N.Y 2025)
  - Querying a FISA §702 database is a separate 4th Amendment search
  - Will generally require a separate warrant
- *United States v. Payne*, No. 22-50262 (9th Cir. 2024)
  - Continues Circuit split on compelled unlocking of smartphone
  - Forcibly placing thumb on phone held no violation of 5th Amend.
  - Separate line of cases on compelled disclosure of passwords also split
- *United States v. Zelaya-Veliz*, 94 F.4th 321 (4th Cir. 2024)
  - Court suggests temporal requirements may cure overbreadth challenges in social media warrants

"Apply" Slide

- Identify progeny of *Loper* and how it might impact your company
- Identify contracts that include cybersecurity requirements, then
  - Review adequacy of controls
  - Ensure staff is properly trained and aware of internal alerting processes
  - Check compliance at regular intervals and remediate as required
- Review the use of AI within your organization
  - Determine whether appropriate AI safeguards are in place
  - Ensure workforce is aware of permitted/unpermitted uses of AI
  - Review and update guidance frequently to keep pace with changes

Cybersecurity Disclosures

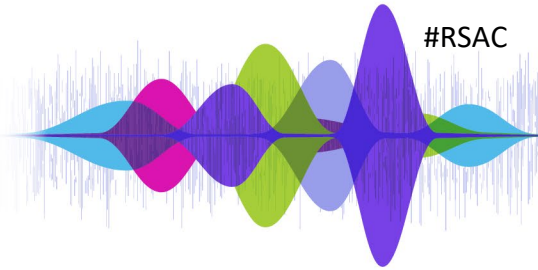
SEC v. SolarWinds Corp. and Brown, No. 1:23-cv-9518 (S.D.N.Y. Oct. 30, 2023)

- Facts of the case
  - The SEC filed charges against SolarWinds and its Chief Information Security Officer (CISO). The SEC accused SolarWinds and its CISO of inadequate cybersecurity practices and misleading disclosures related to a significant cyberattack.
- Issue: Could the SEC expand the Securities Exchange Act's "internal accounting controls" provision to encompass an issuer's cybersecurity controls, or use the "disclosure controls and procedure" provision where disclosure controls existed and systematic failures were not alleged?

Holding

- The U.S. District Court for the Southern District of New York on July 18, 2024, dismissed most of the SEC's landmark cyber enforcement litigation against SolarWinds and its CISO.
- Only a subset of the SEC's material misrepresentation claims, which were associated with the Security Statement published on the Company's website, survived.
- Takeaway: While the court was disinclined to expand the SEC's authority in the cybersecurity context here, companies should still carefully evaluate their cybersecurity posture, closely review all public statements and avoid generalized disclosure relating to cybersecurity to avoid regulatory scrutiny.

Liability of Cyber Professionals



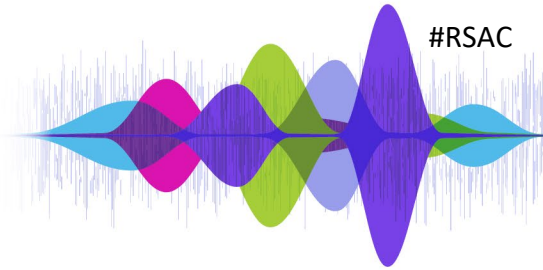
United States v. Sullivan

- Facts of the case
- Issue: Does the Computer Fraud and Abuse Act (CAFA) § 1030 permit a company to later ratify access that was initially unauthorized (e.g., through a Bug Bounty)?

Holding

- No (but Sullivan is seeking rehearing en banc and/or cert)
- Generally a computer owner determines what access is "authorized." *LVRC Holdings LLC v. Brekka.* Sullivan argued that CAFA does not limit when a computer owner may authorize that access.
- Ninth Circuit rejected this, ruling **categorically** that "[i]n [CAFA], 'without authorization' modifies the present tense verb 'accesses'" and thus that **"[a]n actor's authorization**, or lack thereof, is **assessed at the moment of access**."
- **Takeaway: Worst possible holding on this issue because the categorical rule calls into doubt many Bug Bounty programs**
- Sullivan is seeking amicus support for rehearing

Attorney-Client Privilege



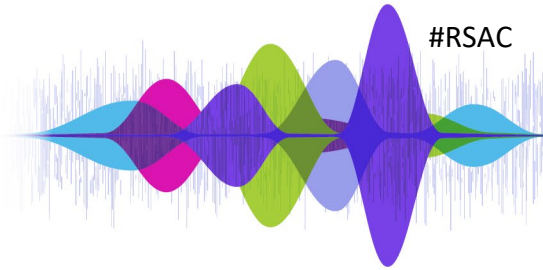
In re Samsung Breach Litigation

- Facts of the case
- Issue: Whether attorney client privilege and work product doctrine apply to documents prepared by a third-party cybersecurity firm retained by Samsung's attorneys.

Holding

- PowerPoint presentations, a one-page Cloud Host Analysis, and an FBI update prepared by the cybersecurity firm were determined to be non-privileged. A draft memorandum was determined to be privileged.
- Takeaway: When engaging third-party consultants, consider the documentation generated and how it is used and distributed both internally and with third parties, such as the FBI.

Reimbursement of Fraud Victims



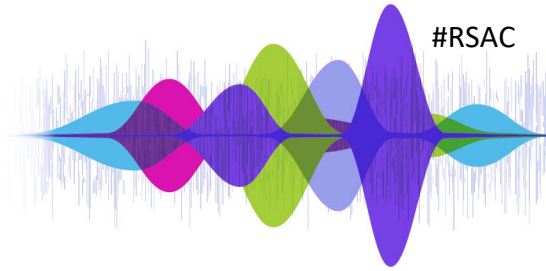
New York v Citibank NA, U.S. District Court, Southern District of New York, No. 24-00659

- Facts of the case
- Issues:
  - Whether the Electronic Funds Transfer Act (EFTA) applies to fraudulent wire transfers initiated through online banking
  - Whether intrabank "consolidation" transfers used in fraud schemes are covered by EFTA
  - Whether Citibank's security protocols and customer agreements violated various federal and state laws
  - Whether state cybersecurity laws (NY SHIELD Act) are preempted by federal law

Holding

- Southern District of New York ruled that the New York AG's core EFTA claims to survive Citibanks's MTD while dismissing state law claims that were preempted by federal law or otherwise barred.
- Takeaways:
  - Review and update customer agreements to ensure compliance with EFTA
  - Implement robust fraud detection for both external transfers and internal account movements
  - Review security-related marketing materials and customer communications

Recent Cybersecurity Enforcement Actions



Security Outside the Core

- Vendors and Suppliers (*AT&T)*
  - New CPRA requirements
- Shadow IT
- Insider Threats
  - North Korean Workers
  - Least Privilege (*Ring*)

User Security

- Email and Account security (*Equiniti*)
- Account takeovers
  - *Citi*
  - *Meta*

Security Outside the Core
Vendors and Acquisitions

AT&T (Sept. 2024 / $13M settlement):

- *Overview*: Vendor misconfigured cloud resource with customer data publicly accessible. While vendor was subject to written security program and contractual provisions, diligence does not appear to have been done and deletion was not confirmed after program termination.
- *Affected Data*: line count for all impacted customers, and bill balance and payment information and rate plan name and features.
- *Number Affected*: 8M

Marriot (Oct. 2024): Marriot agreed to pay *$52 million* to nearly every US state, and *improve its data security practices* to resolve parallel investigations by US state attorneys general and the Federal Trade Commission over its 2018 data breach (where an unauthorized third party infiltrated Starwood (a company acquired by Marriot in 2016) in *July 2014 and remained undetected until September 2018*).

- Insufficient data security program, failing to undertake basic security measures including password controls, network segmentation, adequate MFA and timely patching
- Excessive collection and retention of data

User Security
Email Security and Fake Accounts

2022

What happened? A threat actor (pretending to be an employee of the client), instructed American Stock Transfer to *issue millions of new shares* in the client, *liquidate those shares* and then *send the proceeds to an overseas bank*.

What was the effect? A threat actor transferred *~$4.78 million* to bank accounts located in Hong Kong.

What were the security deficiencies? Prior to the incident, Equinity identified mitigation strategies, but it did not take *steps to implement safeguards and procedures* e.g., providing training and/or ensuring call-backs were performed following email instructions from a client.

2023

What happened? A threat actor used *stolen Social Security numbers to create fake accounts*. These accounts *were automatically linked to real accounts*, even though personal information associated with both accounts did not match.

What was the effect? A threat actor *liquidated securities held in the legitimate accounts*, transferring a total of *$1.9 million to external bank accounts*.

What were the security deficiencies? Equiniti's online platform has a default setting that *automatically linked together accounts that shared the same Social Security number* (even if other personal details did not match). Additionally, Equiniti *did not identify the fraudulent transfers*, the bank handling the transfers notified Equiniti.

User Security
Account Takeovers

Citibank: New York Attorney General sued Citibank for allegedly failing to protect and refusing to reimburse victims of fraud.

- Lack of strong online protections to stop unauthorized account takeovers.
- Failing to effectively respond to identity theft red flags.
- Failing to appropriately respond to notifications of fraud by its customers and misleading them about their rights after a hack or funds are stolen.
- Denying reimbursement to victims of fraud

41 State Attorneys General sent a letter to Meta urging 'immediate action' on user account takeovers. The letter asks Meta to do a better job at preventing account takeovers and provide the following:

- Number of ATOs in the past 5 years
- The suspected cause of increase in ATOs
- ATO safeguards
- Current policies and procedures related to Meta's response
- Staffing related to safeguarding the platform against and responding to complaints

“Apply” Slide

- The actions of companies and their corporate officers relating to cybersecurity disclosures and incident response efforts may result in civil and criminal liability from federal and state agencies. It is therefore imperative that companies closely review and pressure-test all disclosures and public statements relating to cybersecurity practices and incidents for accuracy.
- The regulatory landscape is shifting quickly, and companies should regularly review and update customer agreements and disclosures to ensure compliance with federal and state laws.
- Reducing security risk reduces the most legal risk most of the time. Companies should stay on top of security trends and work closely with their technical teams to ensure they follow industry best practices.

RSAC™ 2025 Conference

Many Voices.
One Community.

Julie Bowen

Senior VP, GC, and Corp. Sec'y
MITRE Corporation
jbowen@mitre.org

Rick Aldrich

Cybersecurity Policy & Compliance
Booz | Allen | Hamilton
Aldrich_Richard@bah.com
@AldrichRick

Aravind Swaminathan

Partner
Orrick
aswaminathan@orrick.com
@cyber_swami